# IoT Potential Risks and Challenges

GRIFES / GITI / EPFL Alumni Conference, Lausanne, May 7th, 2015

Stefan Schiller, HP ESP Fortify Solution Architect D/A/CH

# IoT Potential Risks and Challenges

Agenda

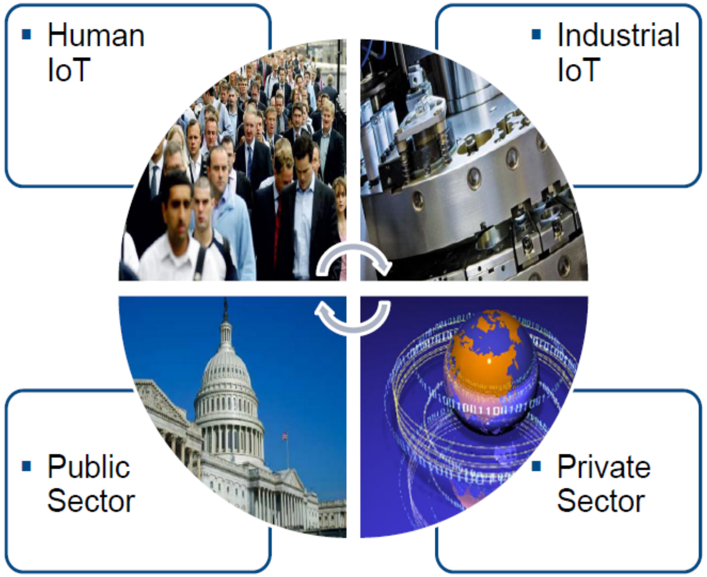
- IDC Directions Summary
- IoT Some Observations
- HP Internet of Things Research Study 2014
- New Industry Standard OWASP Internet of Things Top 10
- Some Players
- Some Architectures
- Existing Means, Tools, Services and Processes for Security Testing of IoT devices
- Challenges

# IDC Direction Summary: Internet of Things (IoT)

## Definition

- It's A Vastly Expanded Set Of 'Things' Connected To The Existing Internet
- It Is Not One Business Model But In Fact Is Millions Of Models
- It Extends The Machine To Machine World To Embrace A Human World
- The IoT Infrastructure Is At The Heart Of The 3rd Platform
- The IoT Will Create Disruption

## Common Segmentation



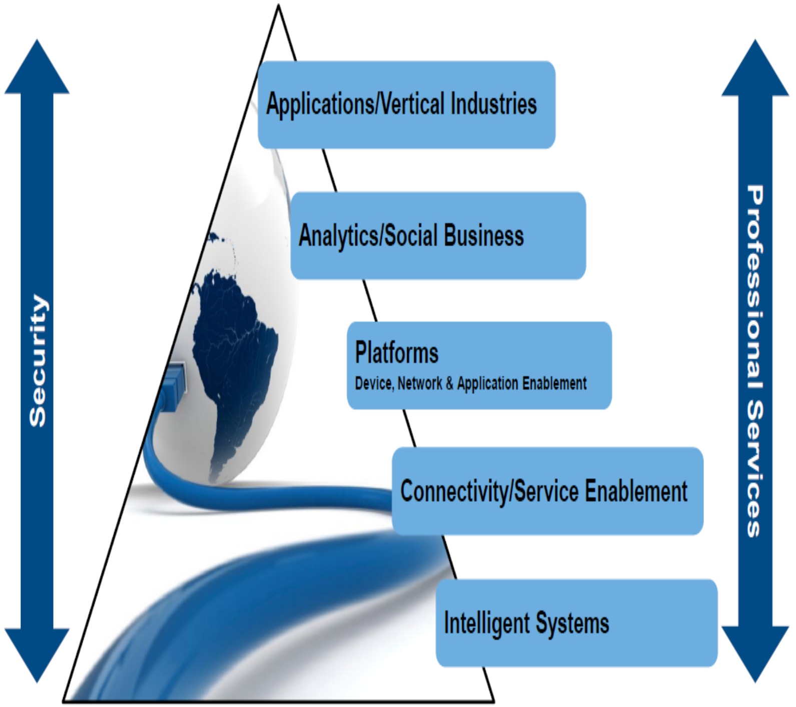
- Human IoT
- Industrial IoT
- Public Sector
- Private Sector

*"IDC defines the Internet of Things (IoT) as a network connecting – either wired or wireless – devices, or 'things', that is characterized by autonomous provisioning, management, and monitoring. The IoT is innately analytical and integrated.*

Source : Summary of IDC conference held on Mar 11-19 at 'Directions 2014'

# IDC Direction Summary: Internet of Things (IoT)

## IoT as an ecosystem



Security

Applications/Vertical Industries

Analytics/Social Business

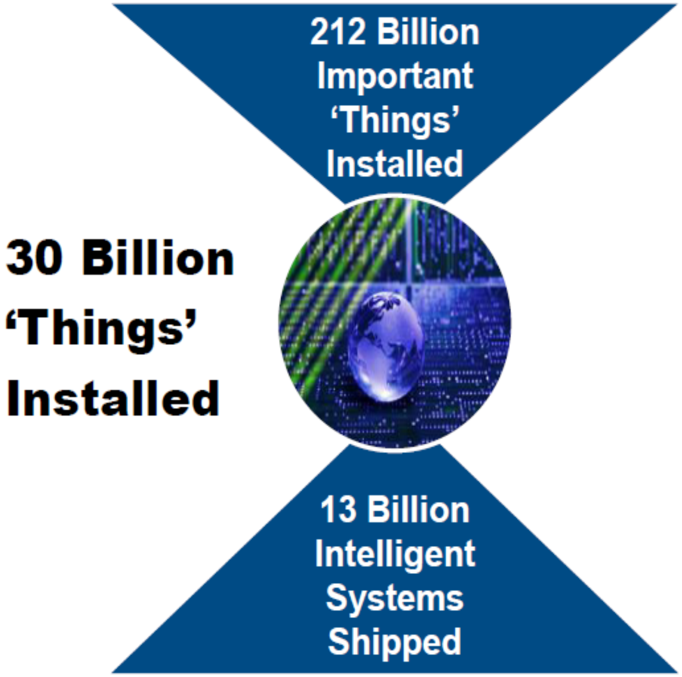
Platforms
Device, Network & Application Enablement

Connectivity/Service Enablement

Intelligent Systems

Professional Services

## IDC's view of IoT in 2020



212 Billion Important 'Things' Installed

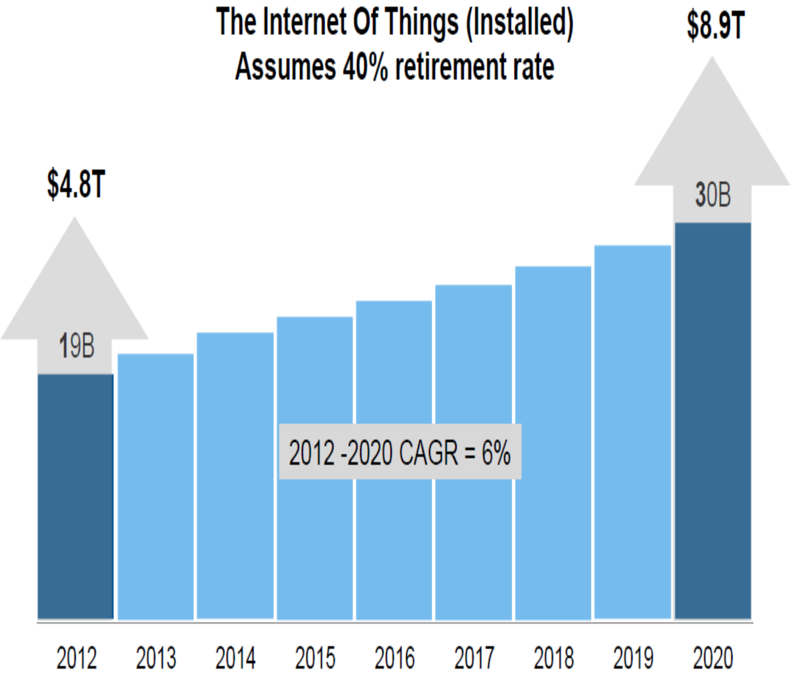
30 Billion 'Things' Installed

13 Billion Intelligent Systems Shipped

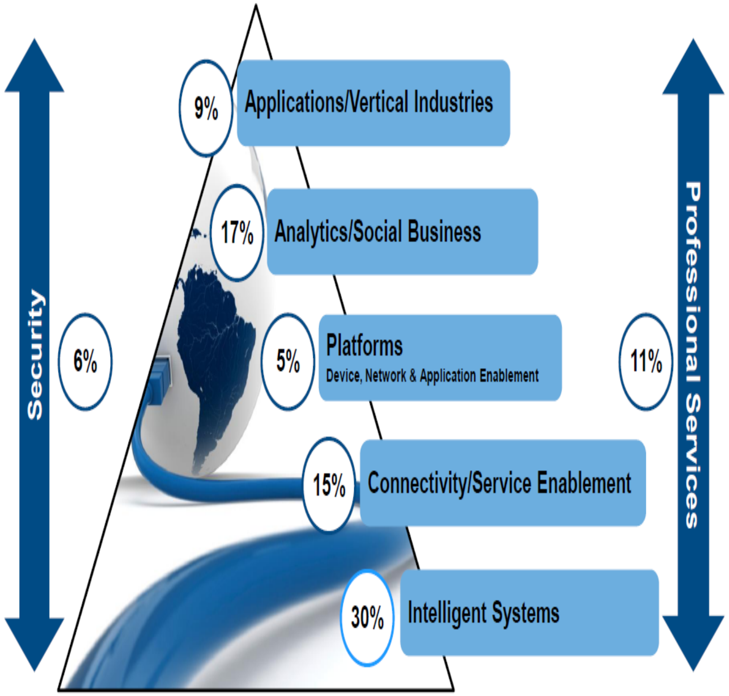
Source : Summary of IDC conference held on Mar 11-19 at 'Directions 2014'

# IDC Direction Summary: Internet of Things (IoT)

## Revenue Opportunity



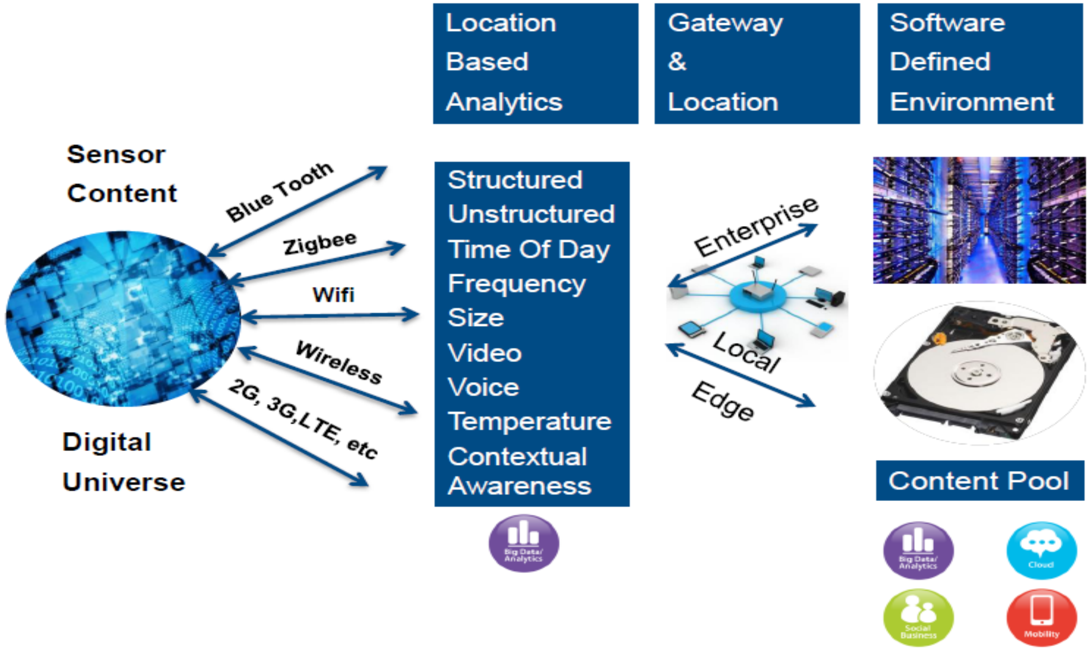
## 2020 – IoT Revenue Path


Security
6%
9%
Applications/Vertical Industries
17%
Analytics/Social Business
5%
Platforms
Device, Network & Application Enablement
15%
Connectivity/Service Enablement
30%
Intelligent Systems
11%
Professional Services

Source : Summary of IDC conference held on Mar 11-19 at 'Directions 2014'

# IDC Direction Summary: Internet of Things (IoT)

## The IoT Impact on IT Infrastructure



Location Based Analytics

Gateway & Location

Software Defined Environment

Structured
Unstructured
Time Of Day
Frequency
Size
Video
Voice
Temperature
Contextual Awareness

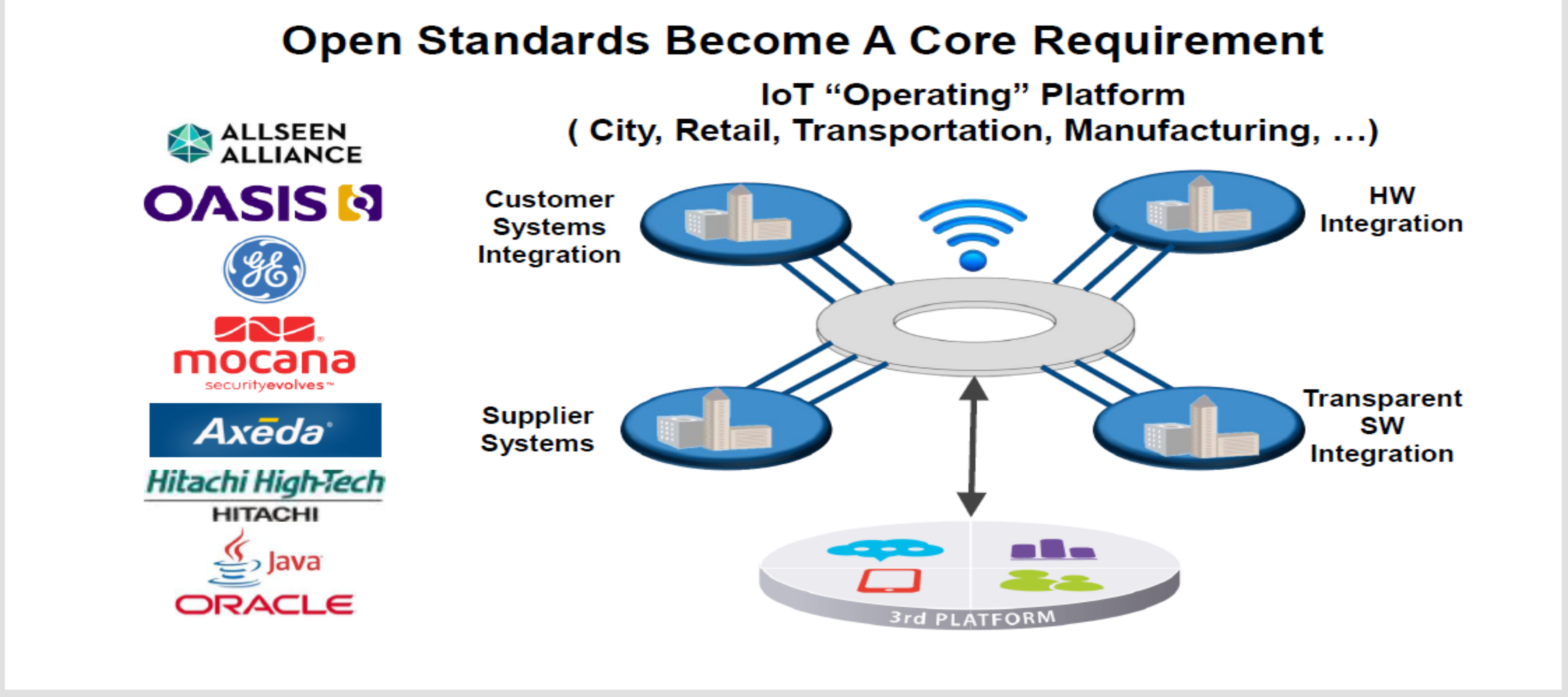
Content Pool

- Security
- Applications
- Software Management
- Virtualization
- Application Management
- Storage Management
- Services
- xSP World
- Next Generation Infrastructure

Source : Summary of IDC conference held on Mar 11-19 at ‘Directions 2014’

# IDC Direction Summary: Internet of Things (IoT)

IoT Partner’s emerge as important vendors



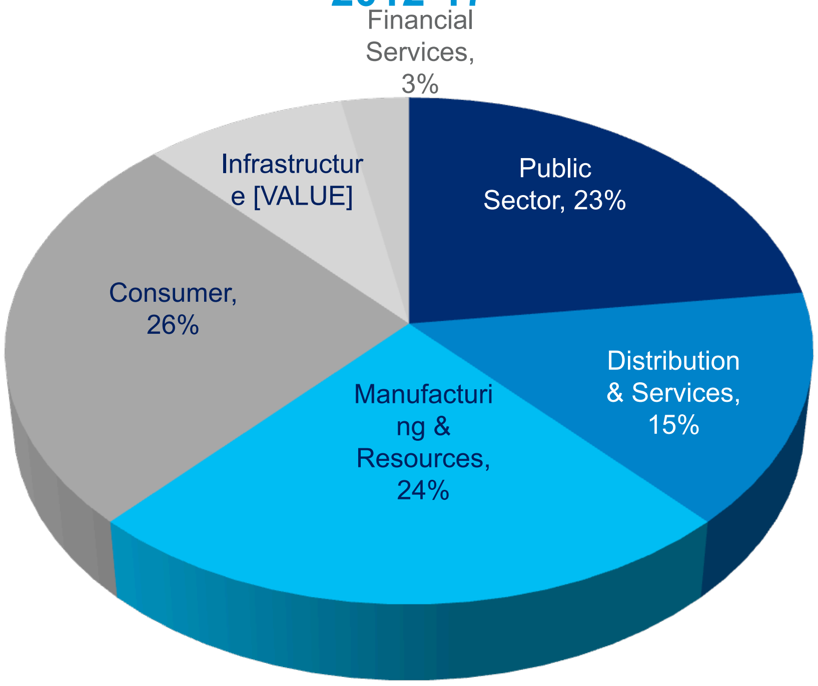
Open Standards Become A Core Requirement

IoT “Operating” Platform
( City, Retail, Transportation, Manufacturing, …)

Source : Summary of IDC conference held on Mar 11-19 at ‘Directions 2014’

# IDC Direction Summary: Internet of Things (IoT)

## WW IoT Spending 2012-17



## Key considerations for IoT Success

**Public Sector**

- Funding
- Where To Start
- Security
- Privacy
- Citizens Buy-In
- Complex Projects
- Collaboration Across Agencies

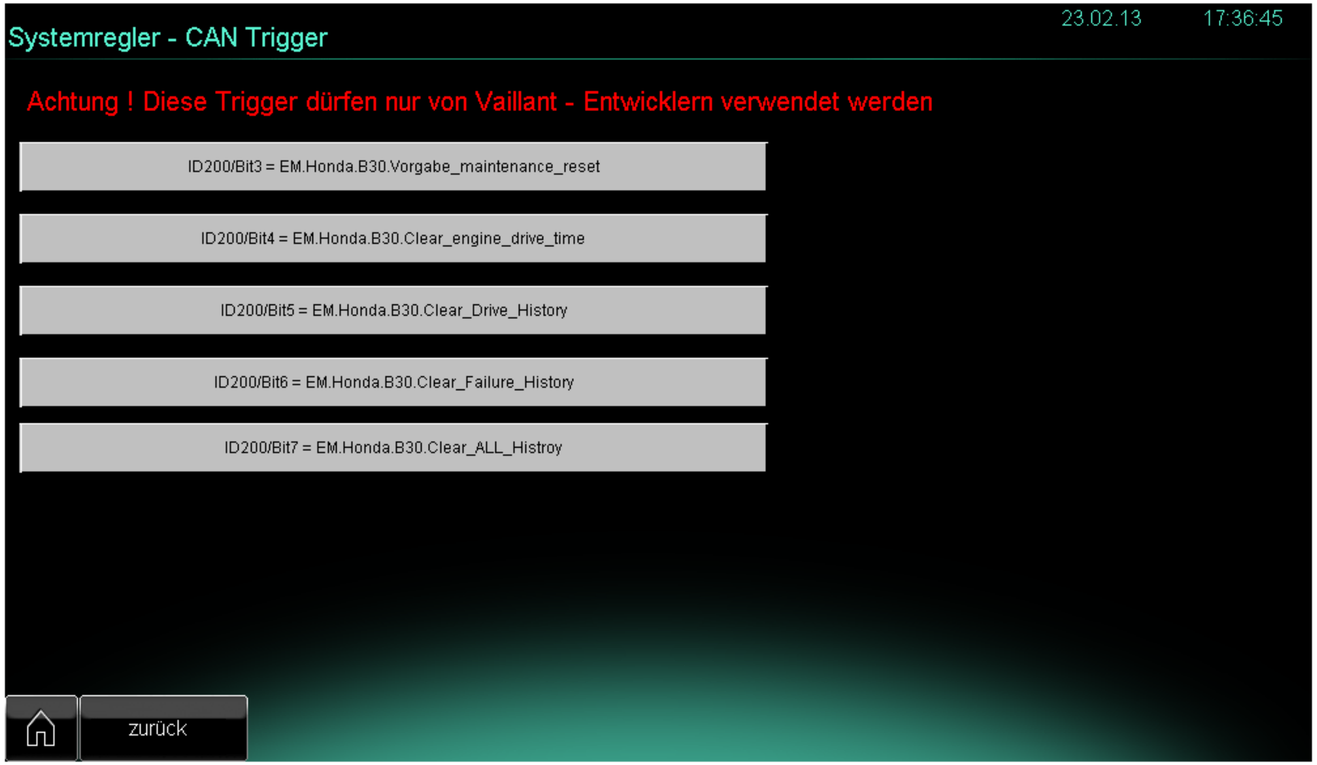
**Private Sector**

- Industry Disruption
- Competitive Differentiation
- Innovation
- Content Ownership
- IT Partnership OT
- Developers

Source : Summary of IDC conference held on Mar 11-19 at ‘Directions 2014’

# IoT Potential Risks: Some Observations, Example 1

Take control over Vaillant eco Power 1.0 Combined Heat and Power Units



Systemregler - CAN Trigger

23.02.13 17:36:45

Achtung ! Diese Trigger dürfen nur von Vaillant - Entwicklern verwendet werden

ID200/Bit3 = EM.Honda.B30.Vorgabe_maintenance_reset

ID200/Bit4 = EM.Honda.B30.Clear_engine_drive_time

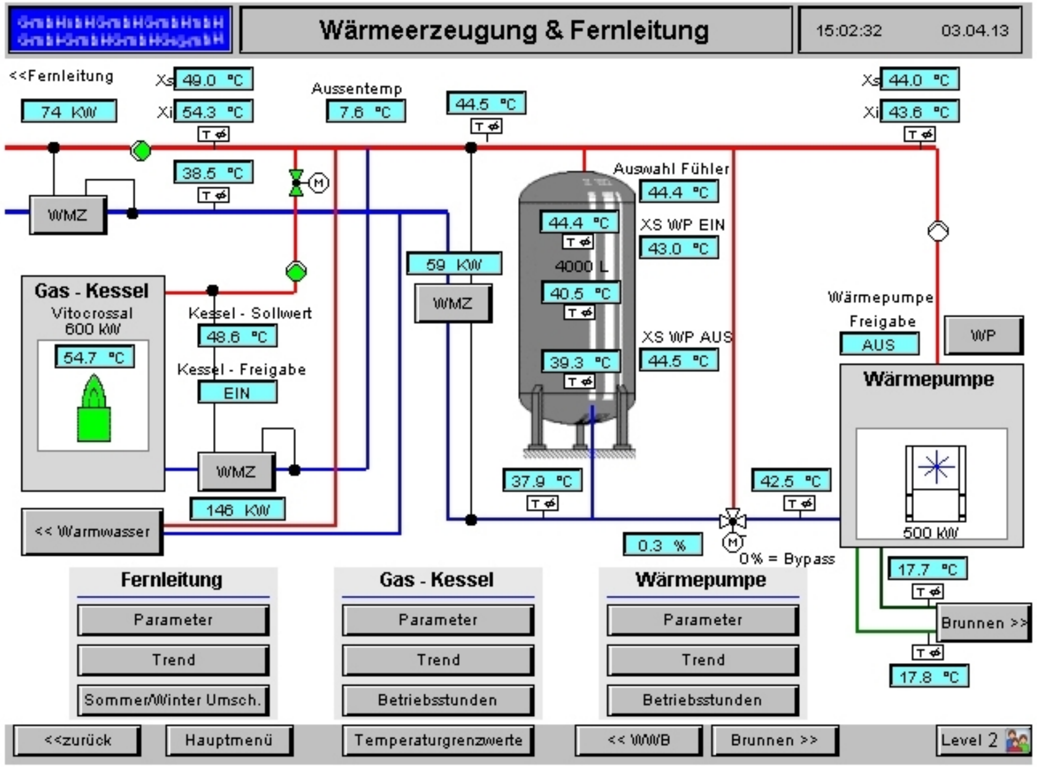
ID200/Bit5 = EM.Honda.B30.Clear_Drive_History

ID200/Bit6 = EM.Honda.B30.Clear_Failure_History

ID200/Bit7 = EM.Honda.B30.Clear_ALL_Histroy

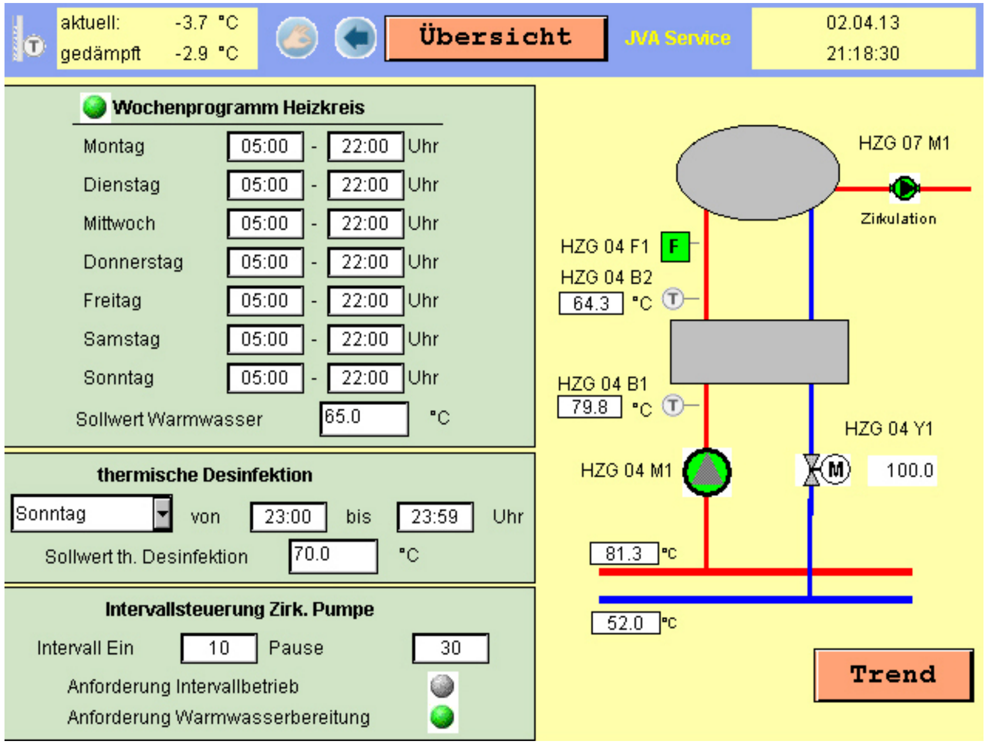
# IoT Potential Risks: Some Observations, Example 2

Take control of Heating Units of a Beer Brewery in the Black Forest



# IoT Potential Risks: Some Observations, Example 3

## Take control of Heating Units of a German State Prison



aktuell: -3.7 °C
gedämpft -2.9 °C

Übersicht

JVA Service

02.04.13
21:18:30

**Wochenprogramm Heizkreis**

| | | | | |
|---|---|---|---|---|
| Montag | 05:00 | - | 22:00 | Uhr |
| Dienstag | 05:00 | - | 22:00 | Uhr |
| Mittwoch | 05:00 | - | 22:00 | Uhr |
| Donnerstag | 05:00 | - | 22:00 | Uhr |
| Freitag | 05:00 | - | 22:00 | Uhr |
| Samstag | 05:00 | - | 22:00 | Uhr |
| Sonntag | 05:00 | - | 22:00 | Uhr |

Sollwert Warmwasser 65.0 °C

**thermische Desinfektion**

Sonntag von 23:00 bis 23:59 Uhr

Sollwert th. Desinfektion 70.0 °C

**Intervallsteuerung Zirk. Pumpe**

Intervall Ein 10 Pause 30

Anforderung Intervallbetrieb ●

Anforderung Warmwasserbereitung ●

HZG 04 F1 F

HZG 04 B2 64.3 °C

HZG 04 B1 79.8 °C

HZG 04 Y1 100.0

81.3 °C

52.0 °C

# HP Internet of Things Research Study 2014

## The Study

- In 2014 HP Security Research took the freedom to review 10 of the most popular devices in some of the most common IoT niches revealing an alarmingly high average number of vulnerabilities (25!) per device. Vulnerabilities ranged from Heartbleed to Denial of Service to weak passwords to cross-site scripting
- HP analyzed IoT devices from manufacturers of TVs, webcams, home thermostats, remote power outlets, sprinkler controllers, hubs for controlling multiple devices, door locks, home alarms, scales and garage door openers
- A majority of devices included some form of cloud service
- All devices included mobile applications which can be used to access or control the devices remotely

# HP Internet of Things Research Study 2014

## The Findings

- On average 25 weaknesses discovered with each device
- 60% of devices that provide user interfaces were vulnerable to a range of issues such as persistent XSS and weak credentials
- 80% of devices along with their cloud and mobile application components failed to require passwords of a sufficient complexity and length
- 90% of devices collected at least one piece of personal information via the device, the cloud, or its mobile application
- 80% of devices raised privacy concerns
- 70% did not encrypt communications to the internet and local network
- 60% did not use encryption when downloading software updates
- 70% of devices along with their cloud and mobile application enable an attacker to identify valid user accounts through account enumeration

# New Industry Standard OWASP IoT Top 10

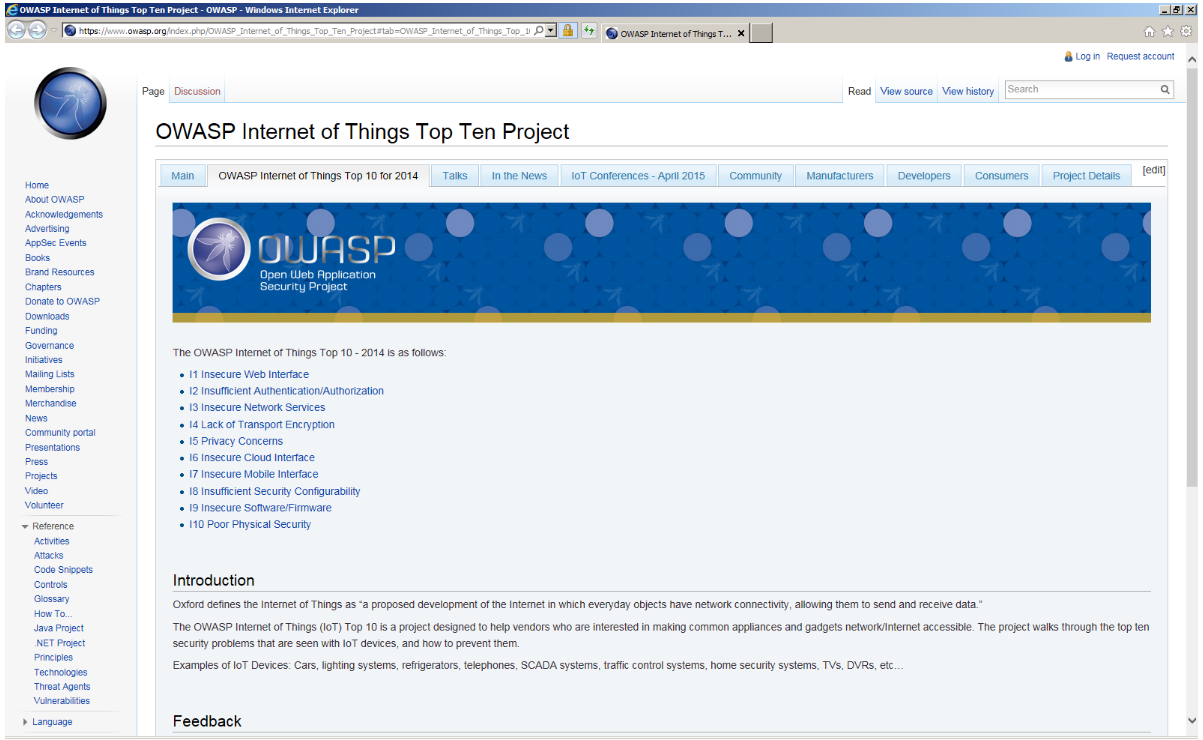
As a consequence to the study HP ESP did help to establish a new OWASP standard

**The OWASP Internet of Things Top 10 - 2014 is as follows:**

- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

# New Industry Standard OWASP IoT Top 10

## The OWASP Project Page



OWASP Internet of Things Top Ten Project - OWASP - Windows Internet Explorer
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_Internet_of_Things_Top_1
OWASP Internet of Things T...
Log in
Request account
Page
Discussion
Read
View source
View history
Search

OWASP Internet of Things Top Ten Project

The OWASP Internet of Things Top 10 - 2014 is as follows:

- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

Introduction

Oxford defines the Internet of Things as “a proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data.”

The OWASP Internet of Things (IoT) Top 10 is a project designed to help vendors who are interested in making common appliances and gadgets network/Internet accessible. The project walks through the top ten security problems that are seen with IoT devices, and how to prevent them.

Examples of IoT Devices: Cars, lighting systems, refrigerators, telephones, SCADA systems, traffic control systems, home security systems, TVs, DVRs, etc…

Feedback

# Some Players

Nest Labs – acquired by Google

Smart Things – acquired by Samsung

Dropcam – acquired by Nest Labs

Revolv – acquired by Nest Labs

# Some Architectures

Nest

- Nest thermostat uses an AM3703 Sitara processor139 from Texas Instruments. The thermostat is based on the ARM Cortex™-A8 architecture. The development tools include the Linux EZ Software development kit and the Android Development Kit for Sitara Microprocessors
- The first-generation Nest OS is based on Linux 2.6.37 and uses other free software components. The firmware image is locked so it only accepts signed firmware updates. Nest also provides unlocked firmware so it can accept unsigned firmware images. This allowed a third party to re-implement the basic logic of the thermostat as an open source project called FreeAbode

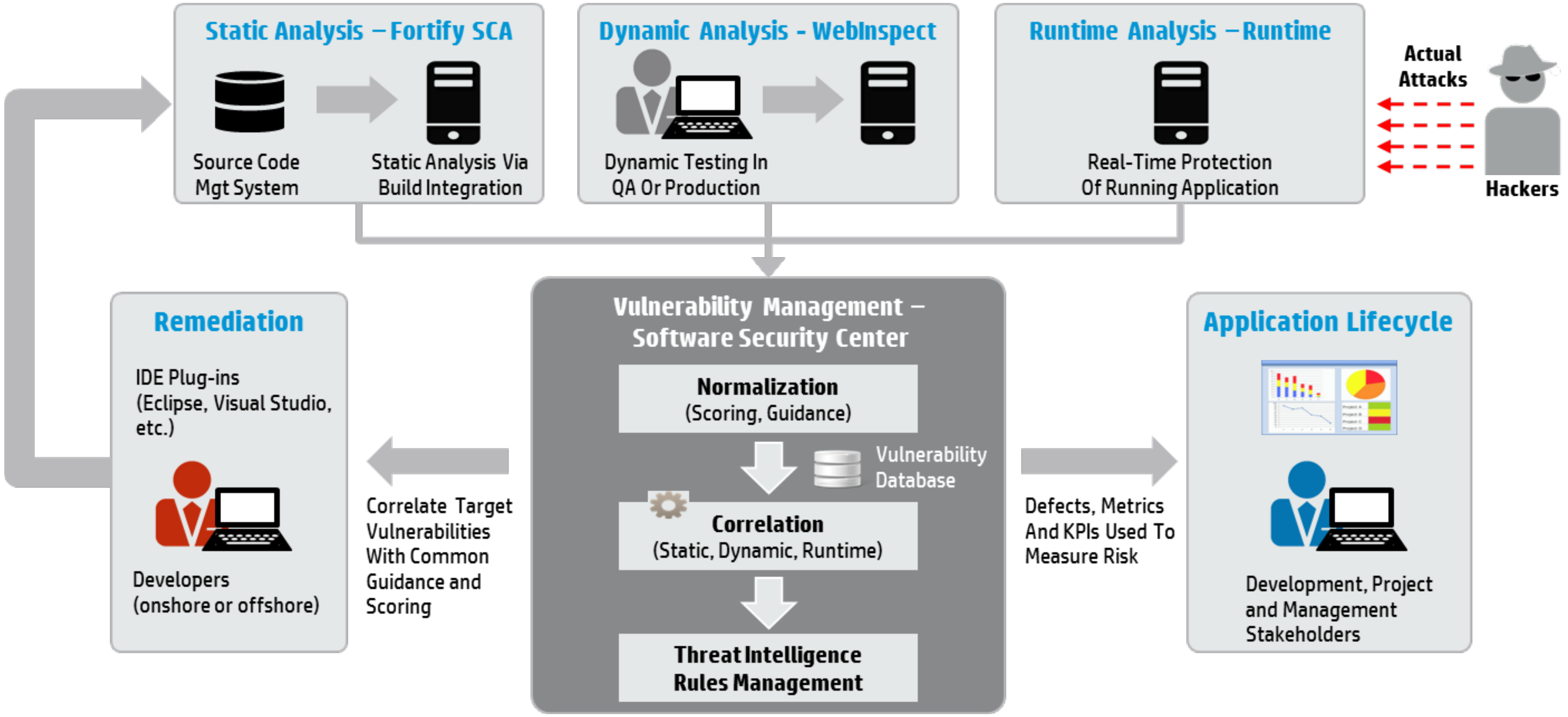
# Some Architectures

Linux/Windows vs. Open-Source Real-Time vs. MBed

- Linux or Windows embedded OS
- Open-source real-time operating systems with a small memory footprint (for example RTOS, Micrium uC/OS-II, uC/OS-III, or TI-RTOS-KERNEL)
- Event-driven MBed OS specifically targeting low-power devices. MBed OS, MBed device server (which acts as an MBed-powered IoT devices cloud aggregator and a portal for Internet applications), and a suite of MBed tools, all Open Source

In general: All these components are well known and well understood and means, tools, services and processes are already in place that CAN be used to invest into IT security of devices in the Internet of Things

# Existing Means, Tools, Services and Processes for Security Testing of IoT devices

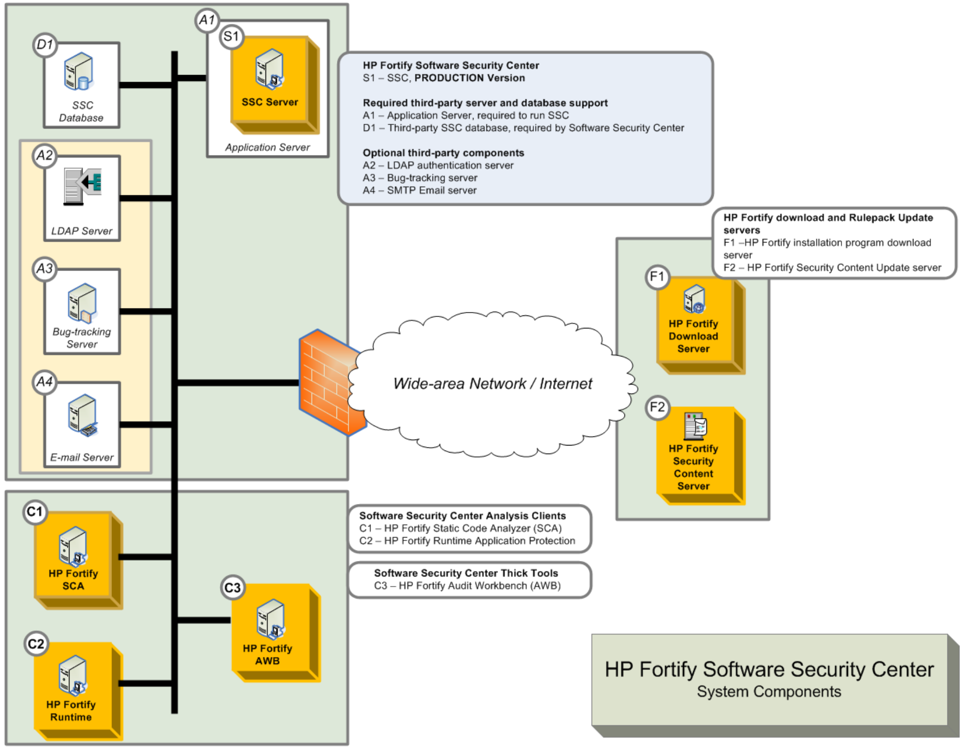


Static Analysis – Fortify SCA
Source Code Mgt System
Static Analysis Via Build Integration
Dynamic Analysis - WebInspect
Dynamic Testing In QA Or Production
Runtime Analysis – Runtime
Real-Time Protection Of Running Application
Actual Attacks
Hackers
Remediation
IDE Plug-ins (Eclipse, Visual Studio, etc.)
Developers (onshore or offshore)
Correlate Target Vulnerabilities With Common Guidance and Scoring
Vulnerability Management – Software Security Center
Normalization (Scoring, Guidance)
Vulnerability Database
Correlation (Static, Dynamic, Runtime)
Threat Intelligence Rules Management
Defects, Metrics And KPIs Used To Measure Risk
Application Lifecycle
Development, Project and Management Stakeholders

# HP Fortify on Premise

## Fortify Software Security Center

- **SCA Static Code Analysis**
- **WebInspect (Enterprise) Dynamic Code Analysis**
- **Fortify Runtime**
  - RTAP Runtime Application Protection
  - RTAL Runtime Application Logging
  - Application View
  - Application Defender
  - WebInspect Agent
- **SSC Collaboration Module**
- **SSC Governance Module**
- **SSC Cloudscan**
  - SCA Scan Step in Cloudscan Server



**HP Fortify Software Security Center**
S1 – SSC, **PRODUCTION Version**

**Required third-party server and database support**
A1 – Application Server, required to run SSC
D1 – Third-party SSC database, required by Software Security Center

**Optional third-party components**
A2 – LDAP authentication server
A3 – Bug-tracking server
A4 – SMTP Email server

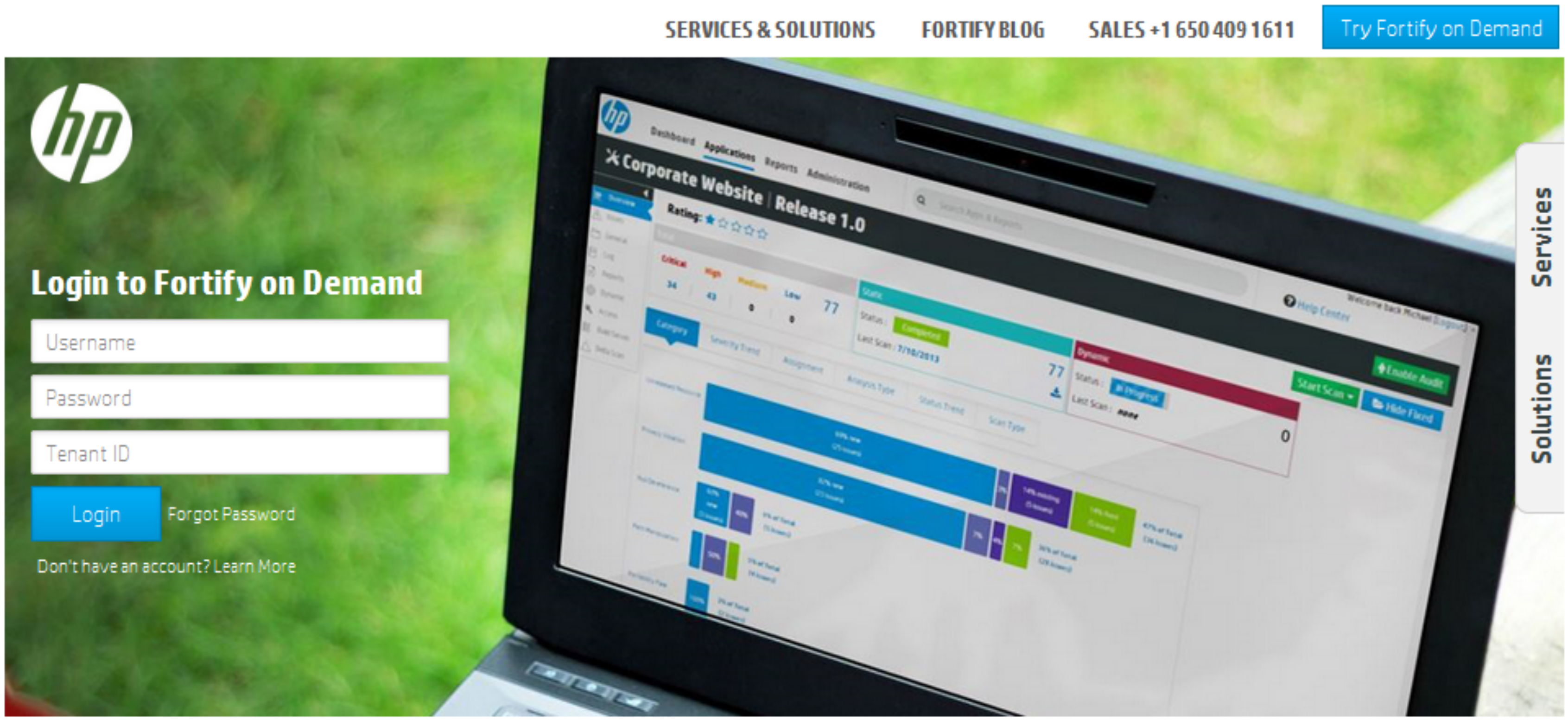
**HP Fortify download and Rulepack Update servers**
F1 –HP Fortify installation program download server
F2 – HP Fortify Security Content Update server

**Software Security Center Analysis Clients**
C1 – HP Fortify Static Code Analyzer (SCA)
C2 – HP Fortify Runtime Application Protection

**Software Security Center Thick Tools**
C3 – HP Fortify Audit Workbench (AWB)

HP Fortify Software Security Center
System Components

# HP Fortify on Demand - Your Tenant in a Public



SERVICES & SOLUTIONS FORTIFY BLOG SALES +1 650 409 1611 Try Fortify on Demand

Login to Fortify on Demand

Username

Password

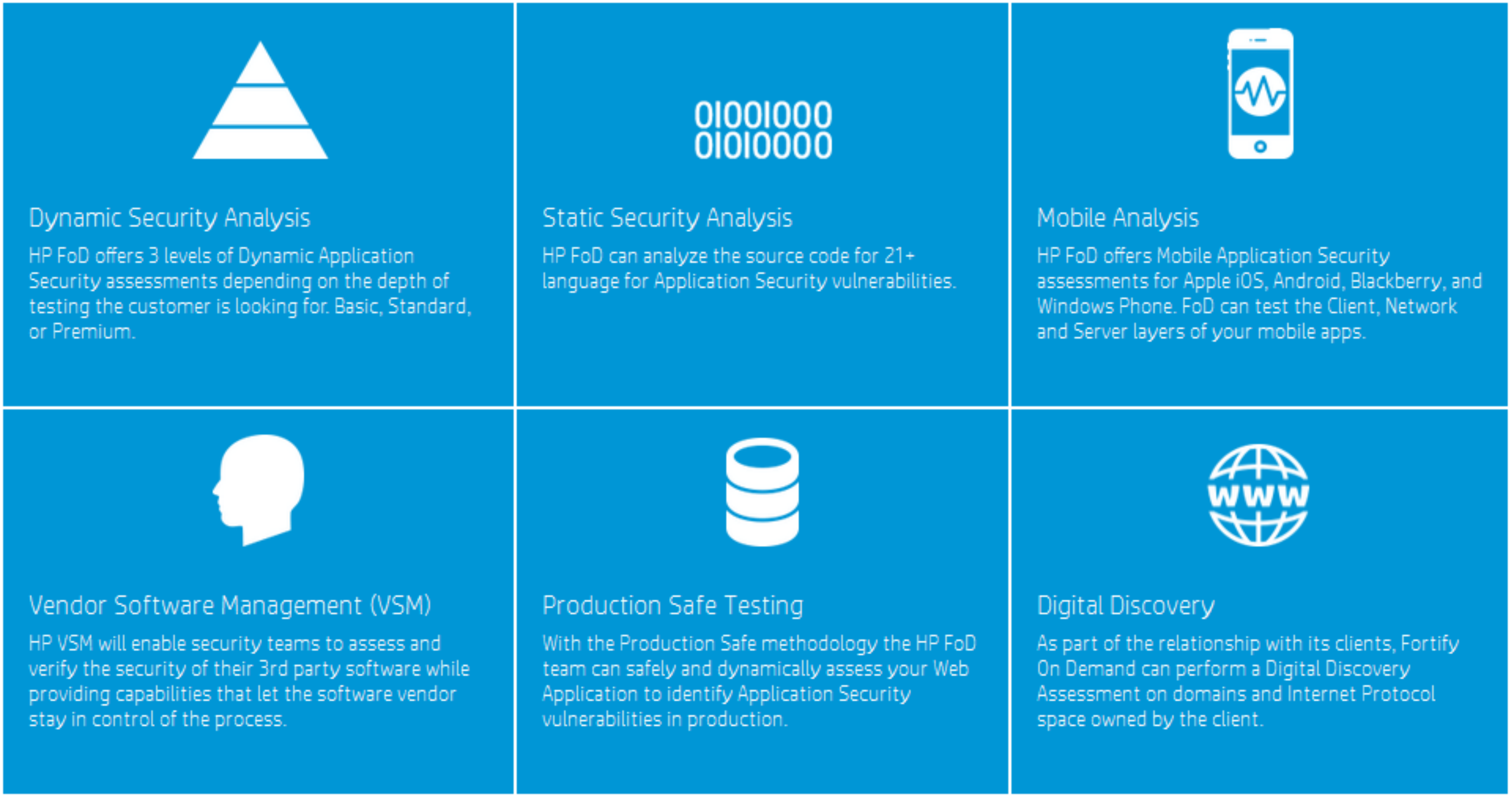
Tenant ID

Login Forgot Password

Don't have an account? Learn More

Fortify on Demand - Your On-demand Application Security Solution

# HP Fortify on Demand - Your On-demand Application Security S



## Dynamic Security Analysis

HP FoD offers 3 levels of Dynamic Application Security assessments depending on the depth of testing the customer is looking for. Basic, Standard, or Premium.

## Static Security Analysis

HP FoD can analyze the source code for 21+ language for Application Security vulnerabilities.

## Mobile Analysis

HP FoD offers Mobile Application Security assessments for Apple iOS, Android, Blackberry, and Windows Phone. FoD can test the Client, Network and Server layers of your mobile apps.

## Vendor Software Management (VSM)

HP VSM will enable security teams to assess and verify the security of their 3rd party software while providing capabilities that let the software vendor stay in control of the process.

## Production Safe Testing

With the Production Safe methodology the HP FoD team can safely and dynamically assess your Web Application to identify Application Security vulnerabilities in production.

## Digital Discovery

As part of the relationship with its clients, Fortify On Demand can perform a Digital Discovery Assessment on domains and Internet Protocol space owned by the client.

# HP Fortify on Demand (FoD)

Get results fast with  security testing software-as-a-service

## Simple

**Launch your application security initiative in <1 day**

- No hardware or software investments
- No security experts to hire, train and retain

## Fast

**Scale to test all applications in your organization**

- Typically 1 day turn-around on application security results
- Support 1000s of applications for the desktop, mobile or cloud

## Flexible

**Test any application from anywhere**

- Secure commercial, open source and 3rd party applications
- Test applications on-premise or on demand, or both

# Challenges

How to convince vendors to apply IT security testing and fix issues found?

- **Infrastructure dealing with heating and/or power generation and/or distribution (Micro CHPs, SCADA, Thermostats, Intelligent Power Meters etc. pp.) can be regarded as critical infrastructures**
- **There are regulations on the way on the EU level as well as on some national levels (e.g. Germany) that will require vendors to prove, that they are spending reasonable effort on IT security of critical infrastructure devices**
- **This should also hold for IoT devices**

- **Raise consumer awareness. Consumers should request from the vendors at least minimum levels of IT security  certification before procuring their devices**
- **This could be implemented via labels like „OWASP IoT Top Ten compliant“**

# Challenges

How to convince vendors to apply IT security testing and fix issues found?

- **Standardization of IoT device platforms**
- **Though there may not be one single platform suited for all the different device types, reducing the number of platforms used per device type would certainly help to ease improving IT security of these platforms while reducing the cost of this effort at the same time**

# Questions?

http://www.hp.com/go/esp

stefan.schiller@hp.com

# Discussion

What are your proposals for improving IT security in the IoT?

-
-
-
-
-
-
-
-
-
-

# Thank you

for having me here
for sharing some of your time with me
for your undivided attention